

NETWORK PENETRATION TEST REPORT



Abertay
University®

Tia

Ethical Hacking 1 - CMP 210

2019/20

Network Penetration Test Report

This report aims to allow the reader to understand what a bad USB is and how they're used in an attack, what attacks are available and the volume of impact they have on a device/network. The paper will demonstrate how to create the scripts for the attacks as well as this it will also demonstrate how to upload the attacks to the badUSB. Finally, this paper will discuss different ways to protect devices and networks against these attacks.

This user guide was created using free to use software, 'Arduino', and a Digispark ATTiny85 USB development board. The arduino software will be used to program the attacks and upload them on to the USB, the Ethical Hacking Lab machines will be the 'victim' PCs and will be wiped before and after each attack to ensure we are not harming anyone's personal computer or breaching the Computer Misuse Act.

It is important that the user understands the gravity of the consequences of deploying a malicious BadUSB, this paper will also discuss the legalities of using BadUSB's for malicious purposes.

I take no responsibility for any consequences incurred by creating a malicious USB, using it on an unauthorised device/system and the aftermath of such an action.

Table of contents

Introduction	4
Background	4
Aim	5
Environment	6
Required Hardware	6
Required Software	6
Arduino Setup	6
Legalities around the badUSB	8
Methodology	9
Uploading the Attack	9
Notepad Attack	9
Fake Update Attack	11
Ransomware Attack	13
Loud Ransomware Attack	15
Fork Bomb Attack	16
Linux Fork Bomb Attack	17
Meterpreter Reverse Shell	20
Countermeasures	23
Software Countermeasures	23
Hardware Countermeasures	23
Logical Countermeasures	26
Conclusion	28
References	29
Appendix	Error! Bookmark not defined.

Introduction

Background

This report will detail the findings of the penetration test that the company has requested, this report will contain detailed descriptions of the methodology used in the test, the overall state of security of the network and countermeasures the company can implement to prevent attackers taking advantage of the highlighted vulnerabilities.

A malicious USB is a USB device that has been deliberately coded to do something else other than it's intended use. These USB attacks work on human curiosity or a malicious actor being able to manipulate multiple people into letting them in to a work place, so they can use the USB attacks themselves on a victim machine. These USB's aren't something many companies think to put into their security campaigns, it gives malicious actors a huge advantage and ability to manipulate this security flaw which can be easily plugged to prevent these types of attacks.

Any USB can be turned into a malicious USB, however, this user guide will demonstrate how to create a 'HID' BadUSB. HID stands for Human Interaction Device, which can be a keyboard or mouse, something that the human user will use to interact with the device. The HID that the BadUSB will 'spoof' is a keyboard and will perform attacks based on this feature. There is a market version of this USB called the Hak5 Rubber Ducky, however it is expensive and is not effective for all types of deployment, there is also an internet-connected version of the Rubber Ducky, called the Cactus WHID, which allows the attacker to upload the attacks remotely.

The Rubber Ducky is expensive, yet exceptionally powerful, however, there is an alternative for almost 10 times less. The Digispark ATTiny 85 is the cheapest alternative to the Rubber Ducky and once the user is confident enough in their own ability, it's almost just as powerful and is more disposable than its expensive counterpart.

Aim

The aim of this report is to explain the findings of the penetration test carried out for the company.

Firstly, the user will learn about the hardware and software aspect of a badUSB and gain an understanding in how they work. The user will learn how to set up the Arduino software for the Digispark hardware, as well as learning the code required to script the badUSB attacks.

Once the user has a base knowledge of the hardware and software of a badUSB, they will then learn about the different types of attacks available and discuss the attacks we will be replicating. There will be an emphasis on the legalities surrounding the attacks and when the legal boundaries are crossed with badUSB's. The user will then begin to code the attacks and test them out in a secure environment.

Once the user has created some attacks, the paper will discuss how these USB's are deployed as part of reconnaissance or a social engineering attack and what happens after the attack has been executed, such as if the attack was built to gain passwords, what the passwords will be used for.

Finally, this paper will also look at how these attacks can be prevented by using various countermeasures in different layouts and how they work, this paper will also look at hardware, software and logical countermeasures, such as write blockers, device control software and how companies prevent these attacks through computer security policies.

Environment

Required Hardware

The main hardware required is the Digispark ATTiny 85 USB development board, the official supplier has currently suspended their stock of the Digispark for the time being, however the USB's can be picked up elsewhere on internet market stores such as eBay and Amazon for cheap and can even be bought in batches.

A machine that has either windows or linux installed is also required, the machine will also require USB ports that are able to read and write, most machines have these ports installed as standard.

Required Software

A virtual machine with at least, Windows 7/Windows 10/Ubuntu or other suitable Linux distribution installed and a workable internet connection is required. This virtual machine will act as the victim PC and means that the user's own computer is not being subjected to various attacks, especially if something goes wrong and it can not be reversed or fixed.

The user will need to install the Arduino IDE first, this software is used to program the USB's attacks. It is important that the following instructions are followed carefully as the setup process can be tricky due to the various steps required to ensure that the Digispark can communicate with the host computer and the Arduino software.

Arduino Setup

Once you have installed Arduino, it is now time to calibrate Arduino properly so that the digispark can download the script correctly.

To be able to run the digispark software with arduino, your computer may need to install additional drivers, they are located within the following file, <https://github.com/digistump/DigistumpArduino/releases/download/1.6.7/Digistump.Drivers.zip>. If it is a 32-bit system being used by the host machine, you

should download and install the file, “Install Drivers”, if it is a 64-bit system however, you should download and install the file, “DPIInst64”.

After the correct drivers have been installed, the user will need to open up ‘Preferences’, this can be found up at the top of the right hand side of the screen. Once this has been opened, the user should be able to identify the text box at the bottom, that reads; “Additional Boards Manager URLs:” - within this text box, the following URL should be entered.

http://digistump.com/package_digistump_index.json

This URL will allow Arduino to download the required digispark board package.

The next step is to open ‘Tools’ and then ‘Boards Manager’ and then go to the drop down menu at the top of the pop-up and select, ‘Contributed’. From this stage, select the Digistump AVR Boards pack, then ‘Install’. Once the pack has installed, navigate back to ‘Tools’ then ‘Boards’, from here Digispark (Default - 16.5mhz) should be selected.

Once these steps have been completed, the arduino IDE is now suitable and ready to start programming with the Digispark.

Legalities around the badUSB

When using a badUSB even as a prank, it is important to consider any laws that surround the use of these USB's. The badUSB can also be used as a part of penetration testing, if this was necessary to test a companies security.

If the badUSB is being created and used for research or 'prank' purposes, it is necessary to understand what the Computer Misuse Act is, if there is not explicit permission from someone to use their machine and the 'attacker' still continues to plug a badUSB in, they would be in breach of the Computer Misuse Act, *"The act makes it an offence to access or even attempt to access a computer system without the appropriate authorisation."* (Sqa.org.uk, 2019).

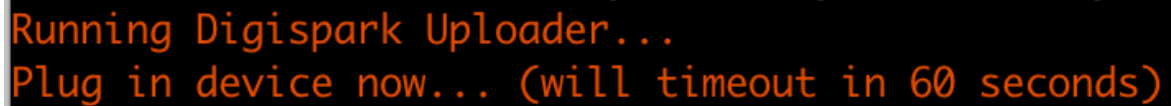
If the attack is going to access several parts of the system, it is important for the victim to know this so that they can give the 'attacker' permission for this. If they do not give permission for the attack to access these parts of the system and the attack still access those areas, the Computer Misuse Act would be breached. *"The act also covers unauthorised access to different parts of a computer system, therefore, a person may be allowed to access one part of a system but not others, and the accessing of the other parts will be an offence."* (Sqa.org.uk, 2019).

In terms of using the badUSB in penetration testing, penetration testers get permission and a scope from the company receiving the penetration test. It is important for the 'pen-tester' to understand how far they can go with their badUSB attack and also has to consider confidentiality and data protection laws such as GDPR and should act within the Computer Misuse Act at all times.

Methodology

Uploading the Attack

Once the attack has been written into arduino, click the upload button which can be found at the top of the window. There will be one minute to insert the USB, once the arduino software has detected the USB, it will begin the upload and will



```
Running Digispark Uploader...  
Plug in device now... (will timeout in 60 seconds)
```

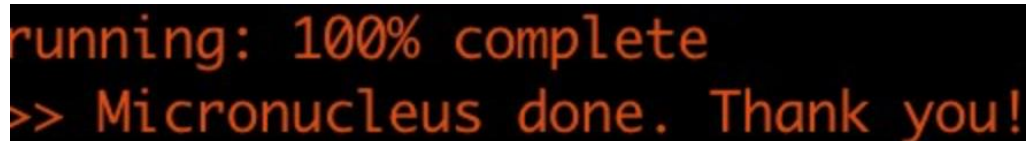
Figure 4. Prompt from Arduino IDE to insert Digispark USB board.

display a success message at the bottom of the screen.

Do not insert the USB before the attack is ready to be uploaded, the payload already loaded on the USB will execute and will not allow the upload to take place.

Notepad Attack

Once the USB is plugged in to the victim's machine, this attack will begin using the 'Run' software which runs a chosen software, this will then open the Notepad



```
running: 100% complete  
>> Micronucleus done. Thank you!
```

Figure 5. Success message from Arduino IDE

application and will type in a message that the attacker has written into the code. This attack will repeat for as long as the USB is attached.

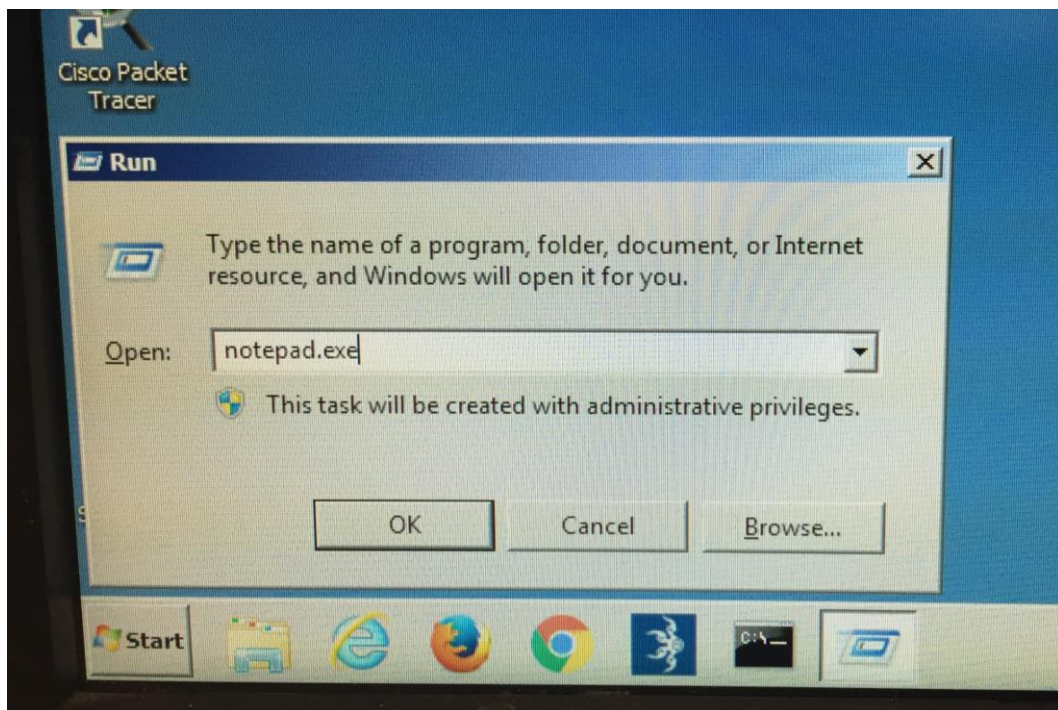


Figure 6. The USB entering in the name of the notepad application.

In a workplace environment, this attack could be used to make a user believe that their PC has an issue and to contact their IT help-desk which a malicious attacker could use to their advantage, within the attack created, the following text is written out:

“Hello, your PC has been found to have an extremely severe vulnerability, please phone the emergency IT Help-desk on 01234 567 890”

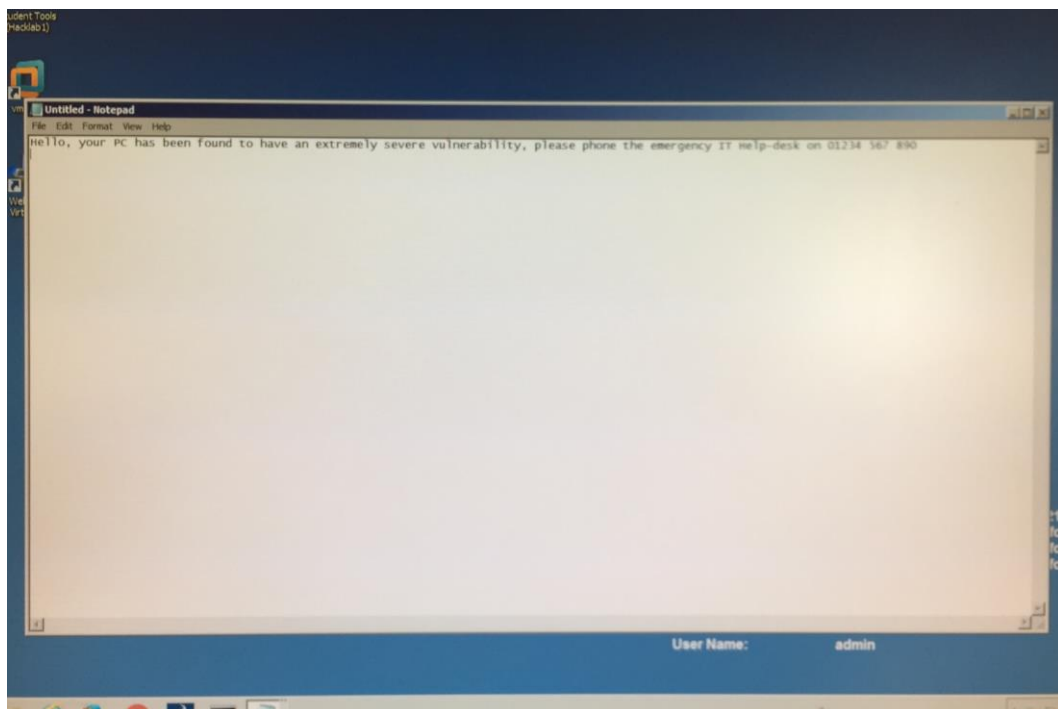


Figure 7. This is the above message written on notepad by the badUSB.

In this example, the IT Helpdesk's 'emergency number' has been changed to the attacker's number, which means when the victim phones the emergency number, it will be the attacker who answers rather than the company's IT department.

The text also states that the vulnerability is "extremely severe" and that the victim should phone the "emergency number", which inevitably causes a sense of urgency and panic within the victim and means they will phone the fake emergency number, without stopping to think about trying to find their companies actual help-desk number or if it's a scam or attack. (See appendix A. for code and video)

Fake Update Attack

This attack makes the victim believe that an update has been activated on their machine. the fake update website contains several OS' and the different versions of each, which means that they can be customised to the victims machine. The attack will load up the required update and display it in full screen in such a way

that the user can't get out unless they know shortcuts on the keyboard or use the windows key.

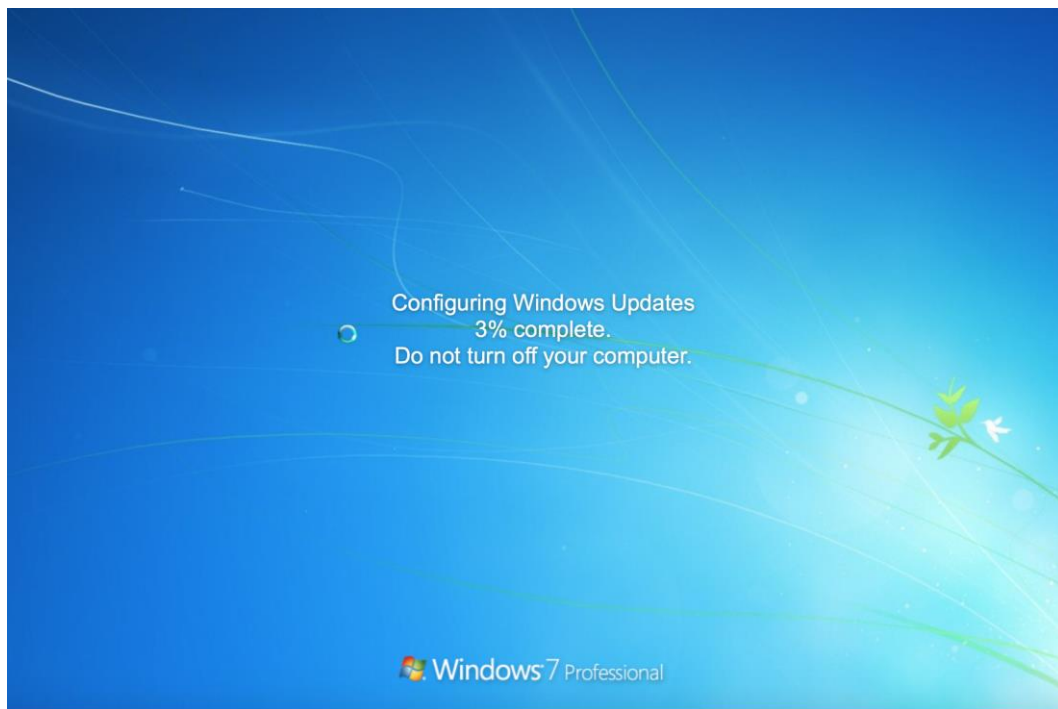


Figure 8. Fake Windows 7 Update from fakeupdate.net

If the user tries mashing buttons, the website will load a 'blue screen of death' for the chosen OS and will effectively make the user believe that their computer has 'died', the machine is still very much alive and this attack causes no damage to the computer unless the machine is shut off abruptly as this may cause damage to files or software.

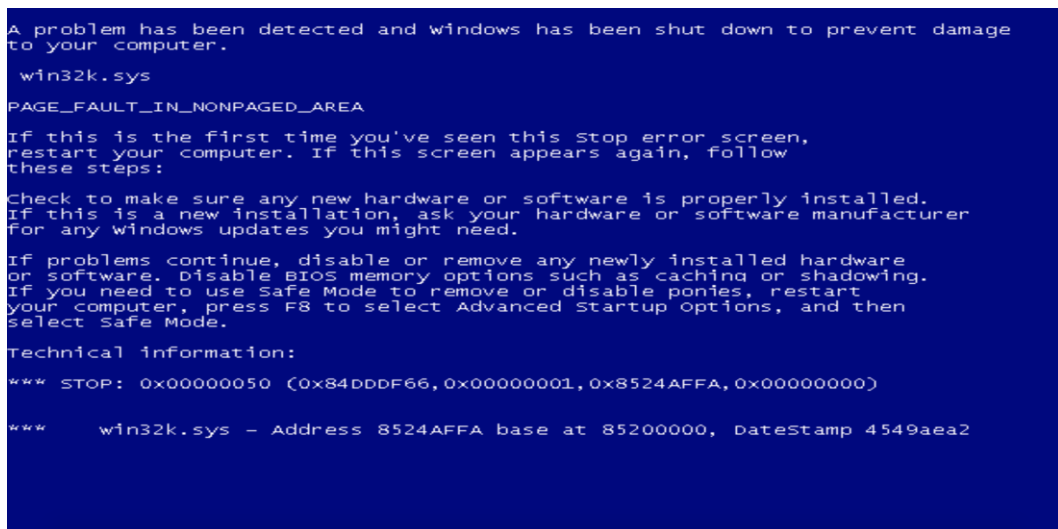


Figure 9. The fake blue screen that follows the 'update'.

This attack is effective if the attacker wants to disrupt a specific victim's activities. The fake update is useful to make the victim believe that they need to wait until the update is finished until they can do anymore work, however, it is possible they will become impatient and mash their keyboard in an attempt to make the computer responsive and load the blue screen instead. This in turn, could possibly cause the victim to either push the power button on their machine or pull the plug, causing them to lose whatever data they had or any progress they had made on any projects. *(See appendix B. for code.)*

Ransomware Attack

Ransomware such as WannaCry and Petya has been detrimental to many businesses and individuals across the world. Ransomware encrypts files so that the victim cannot access them without a 'key' - it is like having all your possessions locked in a chest, which you can't get into without the key and you can't pick the lock or try to break it. The only way back into the 'chest' is through paying the attacker through an anonymous crypto coin wallet, such as bitcoin. "In 2016, the FBI suggested that over \$1 billion was lost to ransomware globally", *(Bunyard, 2019)*.

This attack causes no actual harm to the machine and simply uses internet explorer, or whichever type of browser the attacker chooses. The virus can be

changed to the attacker's choosing, the fake virus that is being used for this attack is Petya, however, cryptolocker and WannaCry can be used too.

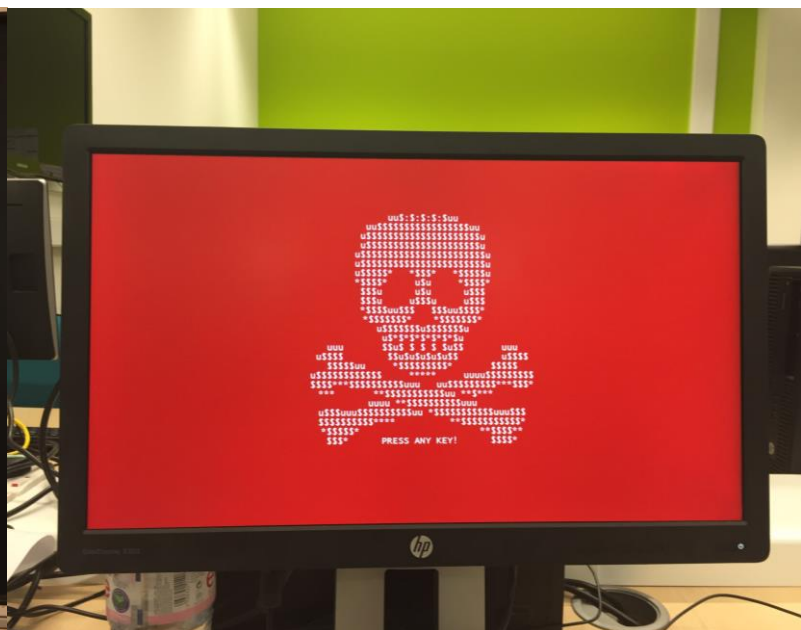
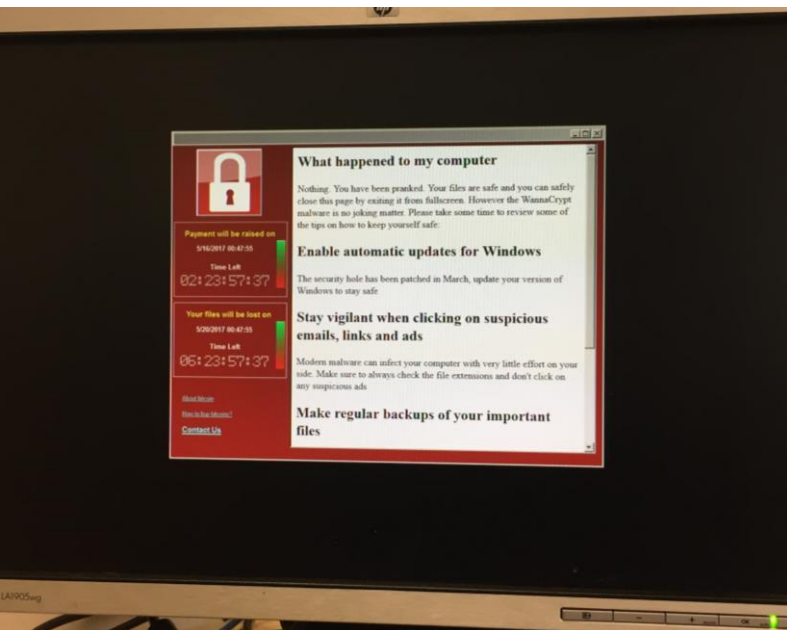


Figure 10. Fake WannaCry attack.

Figure 11. Fake Petya Attack (Flashes grey and red)

This attack does not load any



Figure 12. The Petya Ransomware page.

ransomware on to the victim's machine, it simply mimics a ransomware attack on an internet browser, it is similar to the fake update attack and also loads the website in full screen, but the effects of this attack by a malicious actor are much greater.

This attack can be used in an attack if the attacker is looking to disrupt the full companies activities. Due to the severity of ransomware within a company, it is likely that the company would try to limit how far the ‘virus’ would reach if it is a WannaCry attack as it is a ‘worm’ virus, which will affect each computer on the network, if it is a Petya/CryptoLocker, it is likely they will still shut the network down to isolate the virus’ effects.

The attacker can use this to test a business’ reaction to such an attack and if there are any backdoors in their reaction that they can utilise to their advantage if they plan on leading a large ransomware attack. It can also be used to disrupt the business’ activities, this can have a large knock on effect to their profits and services depending on the size of the business. *(See appendix C. for code)*

Loud Ransomware Attack

It is possible to mimic a ransomware attack and also include a song or sound effect with it. It is the same code as the ransomware attack and is simply an added URL that contains the link to the chosen song or sound effect.

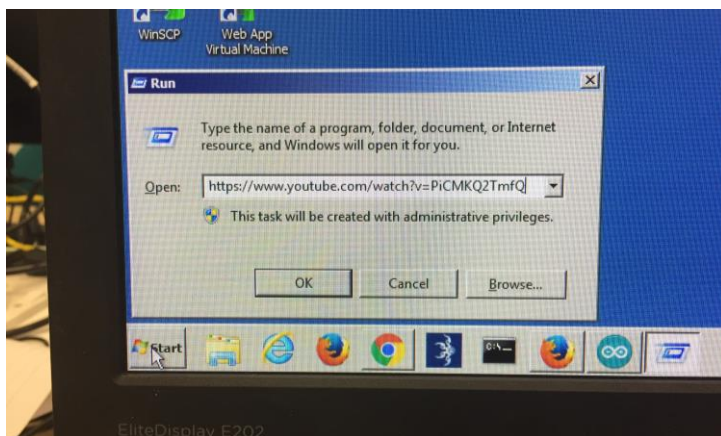


Figure 13. BadUSB entering the YouTube link

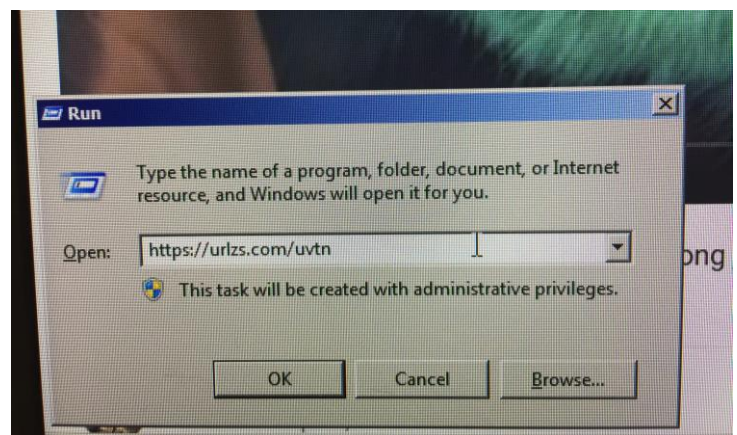


Figure 14. BadUSB entering the website link after opening the YouTube video.

The website can be changed and the song can be changed for a different song or even sound effects, to create a more convincing loud ransomware attack. The current attack could be changed to create a different or desired effect. For this version of the attack, we have decided to stay with Petya and choose a loud and distracting sound. It will still have the same overall affect as the Ransomware Attack, but with added disruption as long as they don’t have any external

speakers/headphones as they will be unable to stop the music/sound effects. (See appendix D. for code and video)

Fork Bomb Attack

DO NOT USE THIS ATTACK ON A MACHINE THAT YOU DO NOT OWN OR HAVE PERMISSION TO USE. THIS ATTACK CAN SERIOUSLY DAMAGE THE VICTIM'S FILES AND OTHER SOFTWARE, USE A VIRTUAL MACHINE TO TEST THIS ATTACK.

A fork bomb attack is a type of attack in which a command that tells the computer to create a batch file and run this batch file, which creates an infinite loop with batch files that keep executing the same request to open a batch file. The CPU tries to deal with these requests but inevitably cannot, which leads to the machine being rendered unusable and crashing.

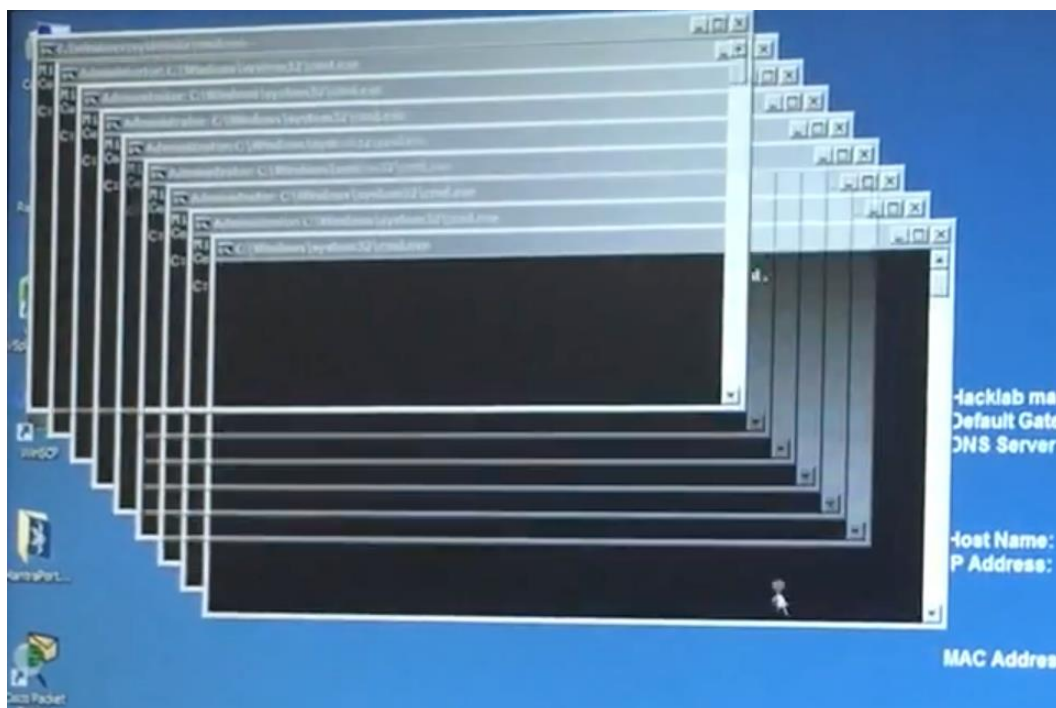


Figure 13. Windows Fork Bomb taking place.

The fork bomb in this attack works slightly differently in the way that it does not open batch files, but opens a command prompt window and replicates itself over and over, until the machine locks itself down or decides to crash. This attack works just as well as a batch fork bomb would, it is just a different way to run this

attack. The USB can be removed after the fork bomb has started, this means that many machines can be attacked in a few minutes, thus expanding the level of disruption and mayhem caused.

This attack is effective if the attacker wants to disrupt the victim's systems and cause chaos, however it does not have any information gathering abilities as the system's memory and resources will be overloaded by the fork bomb, which inevitably means there is no way to access data or memory on the computer while the attack is active, it is possible that the attacker could develop this attack that it becomes a worm and replicates itself on nearby machines on the network and so on.

Through this attack, the victim cannot do anything with the machine as it is and is required to physically turn off their computer to stop the loop, however, if the USB is still attached, the loop will continue to run. Through physically turning their machine off, they will lose any data or files that were currently open and being edited. *(See appendix E. for code and video)*

Linux Fork Bomb Attack

DO NOT USE THIS ATTACK ON A MACHINE THAT YOU DO NOT OWN OR HAVE PERMISSION TO USE. THIS ATTACK CAN DAMAGE THE VICTIM'S FILES AND OTHER SOFTWARE, USE A VIRTUAL MACHINE TO TEST THIS ATTACK.

This attack works the same as the windows fork bomb attack but is used on a linux operating system such as Ubuntu. With this attack, we are having to use the terminal and create a bash script rather than using the more famous command of “:(){ :|:& };;”, this is due to the DigiKeyboard library not accepting some of the characters used in the command.

For this attack we are making a directory, moving to the new directory, creating a txt file called badUSB, entering in the fork bomb commands, changing the permissions on the new txt file and running the fork bomb. This is easy to do

through the terminal and does not need the **USB** to remain attached to the

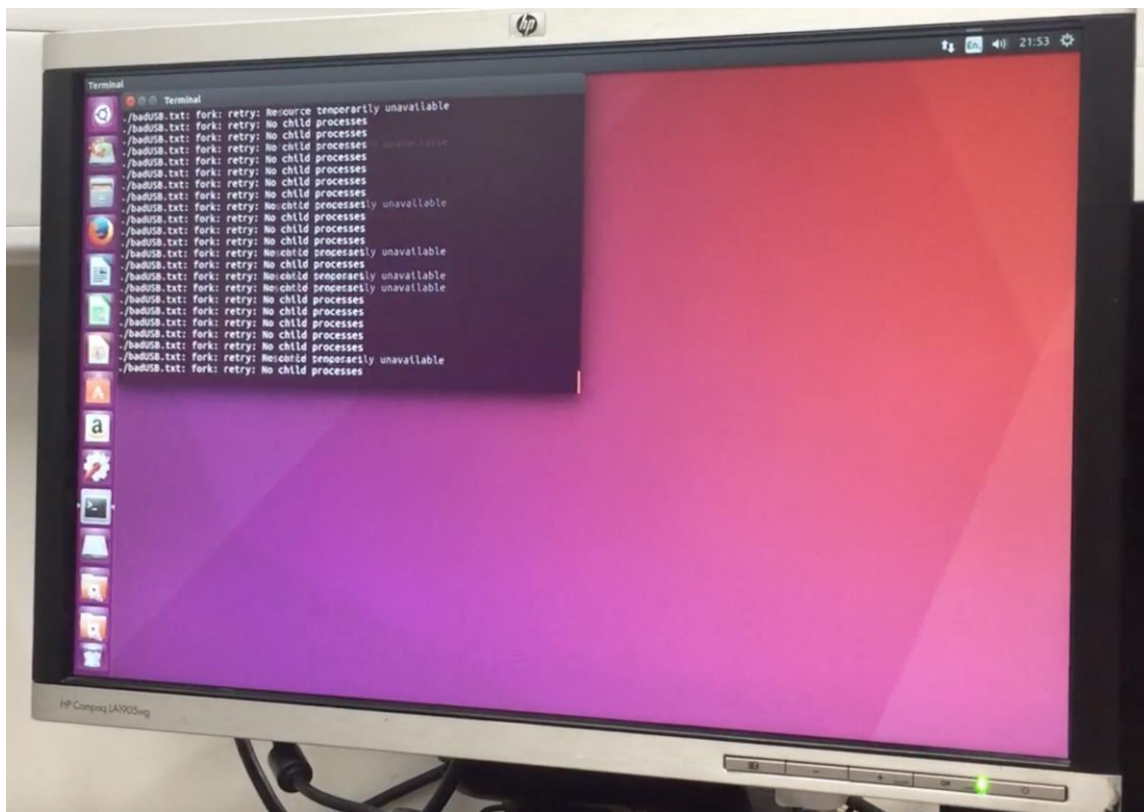


Figure 14. Ubuntu Fork Bomb executing.

computer after the fork bomb has started.

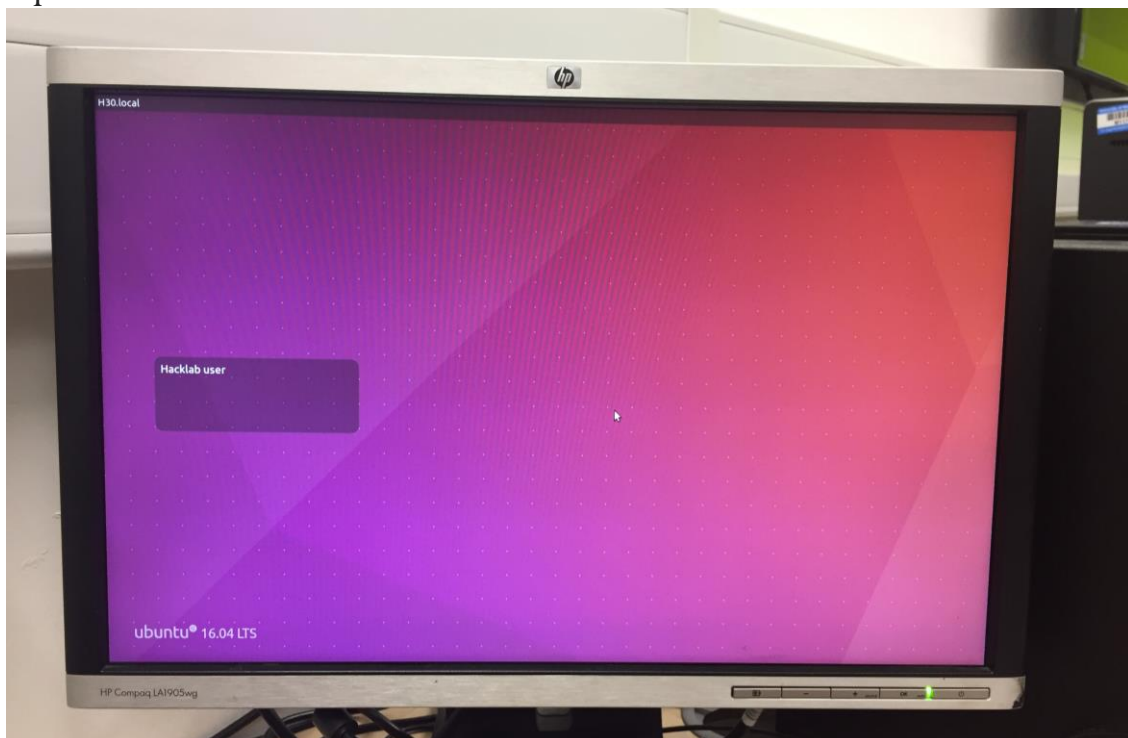


Figure 15. Ubuntu after fork bomb has activated, can't log in or turn machine off using UI.

As with the windows fork bomb, the machine's system will start to slow down and dedicate its CPU power to the fork bomb, this means the victim won't be able to do anything with the machine and will eventually have to manually be shut off either by holding the power button down or pulling the power from the machine.

This attack is effective if the attacker wants to cause mayhem and disruption on a victim or multiple victim's machines. It is possible that the attacker can use a single badUSB on many machines in a small space of time and could even utilise a handful of badUSB's and increase the volume of disruption caused, the attacker could also develop their fork bomb to become a worm rather than having to plug their USB into each machine separately. *(See appendix F. for code and video)*

Meterpreter Reverse Shell

DO NOT USE THIS ATTACK ON A MACHINE THAT YOU DO NOT OWN OR HAVE PERMISSION TO USE. THIS ATTACK IS INVASIVE AND CAN COLLECT SENSITIVE DATA ABOUT A USER, USE A VIRTUAL MACHINE TO BE THE VICTIM IN THIS ATTACK.

THIS ATTACK BREACHES THE COMPUTER MISUSE ACT 1990, IF YOU USE IT ON AN UNAUTHORISED MACHINE/WITHOUT SOMEONE'S PERMISSION AND

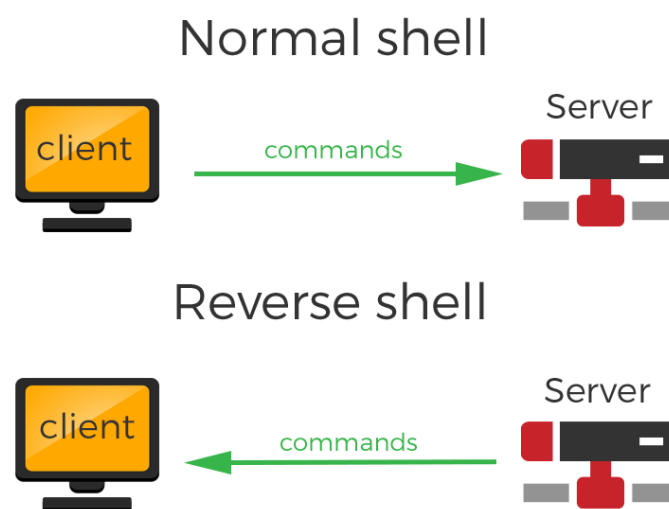


Figure 16. How a reverse shell works.

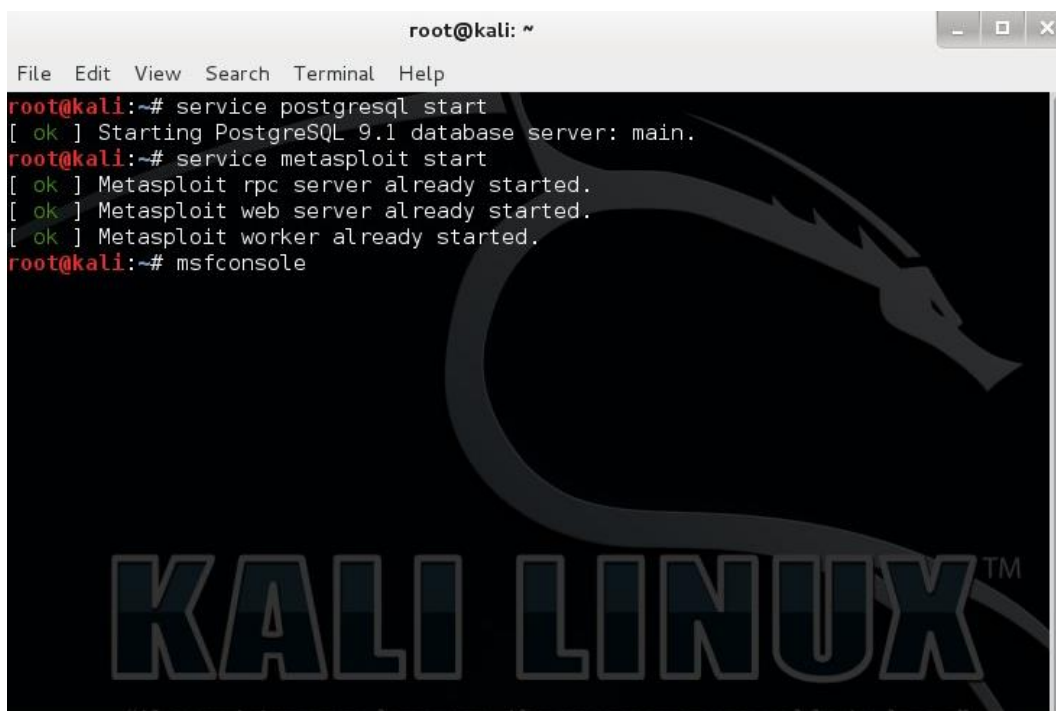
IF YOU USE ANY OF THE DATA OBTAINED THROUGH THE REVERSE SHELL.

A reverse shell attack works by making the victim connect to the attacker, rather than having the attacker connect to the victim, this way the attacker doesn't have

to try and guess what ports are open, all they have to do is specify what ports and IP address they want to use for the victim's machine to connect back to.

These attacks allow an attacker to access a machine and can execute commands through the machine to retrieve usernames and passwords, for emails, wireless connections and user profiles as well as create profiles for themselves, access files that may be private and even delete files as well as logs which will get rid of any trace of them being there in the first place.

This reverse shell attack uses Kali Linux and its Metasploit software, it primarily uses the Metepreter which is housed in Metasploit, then a payload is generated and encoded into 'base64' which means it can be digested by the victim machine. Once the badUSB is plugged into the victim machine, the reverse shell is executed and within a few seconds, the attacker has access to the victim's files, usernames and passwords, this attack is aimed at a Linux OS, but can be tweaked to attack a Windows or Mac OS.

A screenshot of a Kali Linux terminal window. The window title is 'root@kali: ~'. The terminal shows the following commands and output:

```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Metasploit rpc server already started.
[ ok ] Metasploit web server already started.
[ ok ] Metasploit worker already started.
root@kali:~# msfconsole
```

The background of the terminal features the Kali Linux logo, a stylized dragon head, and the text 'KALI LINUX™'.

Figure 17. Kali Linux and Metasploit running on command line.

This attack is an extremely dangerous attack and is different to the rest of the attacks that have been demonstrated, the attacker can get a lot of confidential and valuable data from this attack and can use this for multiple reasons such as

financial gain, general disruption or to simply get more information about the targeted victim/company or of an acquaintance/partner company through the victim's machine.

The attacker can also remove the USB from the machine after the attack has started, the victim is likely not going to realise that a reverse shell attack has taken place as it does not appear on the screen as the hacker begins attacking the machine and stealing passwords, deleting logs, e.t.c. *(See appendix G. for code)*

Countermeasures

The countermeasures that are going to be discussed are not one-hundred percent foolproof and it is possible that some of these attacks can bypass these countermeasures, especially if they have been altered to deliberately bypass them, however, it's more effective to have countermeasures in place and keep them up to date than have nothing at all.

Software Countermeasures

The first software countermeasure is anti-virus software. Kaspersky Labs have recently created a BadUSB blocker and added it to their current 'end-point' anti-virus software which is aimed at businesses, once a USB has been connected to the computer, it will observe how the USB works and if it acts 'suspiciously', it will block the USB, (*Kaspersky.com, 2019*). It hasn't been stated how quickly the USB will be blocked if it acts suspiciously however, it may be quick enough for it to block the USB before it finishes a command.

The second software countermeasure is called 'blacklisting'. It is similar to the process of blacklisting attacker's IP addresses when they are attacking a network, but it is blacklisting the USB instead. This is done by an administrator within their group policies for a network, through this they can block any unusual or block USB's being allowed on the machine, however, this type of method can

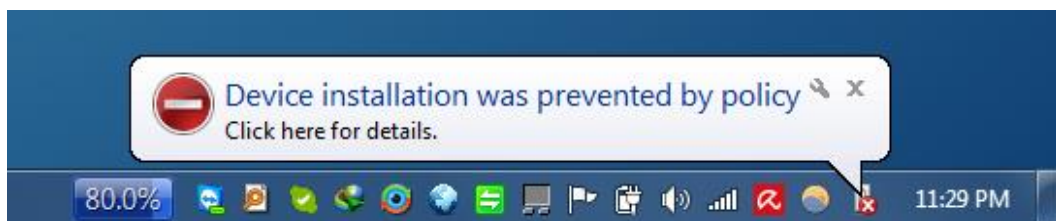


Figure 18. Blacklisting in action against a blacklisted device.

only be used on a Windows OS and as part of a company network.

Hardware Countermeasures

The first hardware countermeasure is USB port blockers. The port blockers are USB heads with small plastic objects inserted in the top, that fit in to empty USB ports and require a key to be removed. They are inserted into empty USB ports that aren't being used for keyboards, mice and other data storage devices.



Figure 19. Lindy USB Blockers - Blue.

They need a specific coloured key to be removed for example, if it is a blue USB block, it requires the blue key to unlock and remove it, this increases the overall security of this product as it means that if the attacker has thought about port blockers and brought a key



Figure 20. Lindy USB Blocker Key - Blue.



Figure 21. USB blocker fitted into computer USB port, same colour key to unlock and remove.

with them, it may not be the correct colour.

Similar to the USB port blockers, the second countermeasure is a USB locker. This device is used to lock keyboards and mice into the machine to prevent theft, on the other hand, they can be used to stop attackers bypassing a blocked USB by pulling the keyboard USB out and inserting the badUSB instead. They also

require a key, however it is not the same type of key as the USB blocker, it is a specific key that the IT administrator will have.



Figure 23.

Figure 22. Kensington USB device and port locks.

Logical Countermeasures

Logical countermeasures are policies and rules set by the company and for an individual it's important to exercise common sense and consider some key rules.

For an individual, a logical countermeasure that they can employ is to not plug in USB devices they don't know or recognise. Many USB's are harmless and probably have files on them that could identify who the owner is, but there is a possibility that a USB could be a badUSB or contain malicious content, this is why attackers may drop USB's with stickers such as 'confidential' or 'sensitive' to grab the victim's attention and toy with their curiosity, leading them to insert the badUSB into their computer.



Figure 24. USB labelled 'Confidential'



Figure 25. USB labelled 'Personal'

Another simple logical countermeasure that can be applied is locking the machine when it is not in use. These attacks cannot take place if the machine is locked as it needs to have access to the unlocked system to use the command line tool and powershell, if the badUSB's attack cannot access these tools, it will simply fail to work. It is possible that they may be able add a brute-force aspect to the badUSB in the future, however, the Digispark does not have the memory or the power to do this at the time of writing.

For companies, they may already have an overhead IT policy in place, this usually outlines their rules on IT and includes sub-policies such as their IT security policy. Many companies employ a removable media policy as part of this, here they can outline what is allowed if removable media is allowed within the workplace and the consequences if the policy is not followed, or it can state that removable media is not permitted at all within the workplace.

It is to the companies discretion whether they allow USB's to be brought in at all, but if they do, they can put preventative measures in place such as, any removable media being brought in needs to be screened by the IT department and can also be 'registered', it can also be that you need to acquire USB's from the IT department that are encrypted and are kept in the workplace. These measures can limit the possibility of badUSB's making their way in without any physical interference by the attacker, these policies may not stop an attacker using social engineering to get their USB's in.

Another countermeasure that businesses can make use of is training their staff about general security and how it can affect them and their workplace, they can become proactive about the dangers the company faces and will be able to

identify possible security vulnerabilities and attacks, for example they will be able to challenge a stranger walking around their offices who is saying they are here for an IT issue and know what the next step is.

Conclusion

The reader of the paper should now be able to identify the types of badUSB available, install the Arduino IDE, create and upload attacks to the DigiSpark ATTiny85 USB Development Board. The reader should also be able to identify the different attacks discussed, the effect it has on businesses and individuals and the countermeasures that can be put in place to prevent and deter badUSB attacks within a business or on an individual's machine.

References

- GmbH, S. (2019). *USB peripherals can turn against their users - Security Research Labs*. [online] Srlabs.de. Available at: <https://srlabs.de/bites/badusb/> [Accessed 12 Feb. 2019].
- Laptopmag.com. (2019). *20 Awesomely Weird USB Gadgets*. [online] Available at: <https://www.laptopmag.com/articles/awesomely-weird-usb-gadgets> [Accessed 12 Feb. 2019].
- Opensource.srlabs.de. (2019). *USB storage - BadUSB Exposure - SRLabs Open Source Projects*. [online] Available at: https://opensource.srlabs.de/projects/badusb/wiki/USB_storage [Accessed 12 Feb. 2019].
- Greenberg, A., Dreyfuss, E., Lapowsky, I., Barrett, B., Newman, L. and Thompson, N. (2019). *Why the Security of USB Is Fundamentally Broken*. [online] WIRED. Available at: <https://www.wired.com/2014/07/usb-security/> [Accessed 11 Mar. 2019].
- Techspirited. (2019). *How Does a Flash Drive Work? We Knew You Wanted to Know*. [online] Available at: <https://techspirited.com/how-does-flash-drive-work> [Accessed 12 Mar. 2019].
- Businessdirect.bt.com. (2019). *BT Business Direct - Kensington USB Port Lock With Blockers (K67913WW)*. [online] Available at: https://www.businessdirect.bt.com/products/kensington-usb-port-lock-with-blockers-k67913ww-CRL8.html?utm_content=QE00&ReferrerID=QE00&utm_source=google&utm_medium=cpc&utm_campaign=pla&utm_content=QE00&gclid=Cj0KCQjwjppjkBRDRARIsAKv-0O0tLx3KXTJUTn07Pz5ZVSwid1bqft56C6ySeyG7Tnt_nC8Y6xhazukaAi9jEALw_wcB [Accessed 12 Mar. 2019].
- Amazon.co.uk. (2019). [online] Available at: https://www.amazon.co.uk/LINDY-USB-Port-Blocker-without/dp/B000I2JWK4/ref=asc_df_B000I2JWK4/tag=googshopuk-21&linkCode=df0&hvadid=309903005216&hvpos=1o4&hvnetw=g&hvrnd=7952834316290794246&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9046870&hvtargid=aud-545671390501%3Apla-338189054866&th=1 [Accessed 12 Mar. 2019].
- Hacker Noon. (2019). *Reverse shell !?!*. [online] Available at: <https://hackernoon.com/reverse-shell-cf154dfee6bd> [Accessed 12 Mar. 2019].

Digistump.com. (2019). *digispark [Digistump Wiki]*. [online] Available at: <https://digistump.com/wiki/digispark> [Accessed 12 Mar. 2019].

Hak5 Forums. (2019). *[payload] Ducky script using mimikatz to dump passwords from memory*. [online] Available at: <https://forums.hak5.org/topic/29657-payload-ducky-script-using-mimikatz-to-dump-passwords-from-memory/> [Accessed 12 Mar. 2019].

Hackingtutorials.org. (2019). [online] Available at: <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/> [Accessed 12 Mar. 2019].

FakeUpdate.net - Fake Windows Update Screens. (2019). *Fake Windows Update Screens*. [online] Available at: <http://fakeupdate.net> [Accessed 29 Apr. 2019].

Quora.com. (2019). *How can pulling a computer's plug while it's on cause damage to the hardware?* - Quora. [online] Available at: <https://www.quora.com/How-can-pulling-a-computer's-plug-while-its-on-cause-damage-to-the-hardware> [Accessed 29 Apr. 2019].

Bunyard, T. (2019). *The Effect of Ransomware on Businesses & Organisations / Cloud Central*. [online] Cloud Central. Available at: <https://cloudcentral.co.uk/effect-of-ransomware-on-business/> [Accessed 29 Apr. 2019].

Vesiluoma.com. (2019). *Exploiting badUSB/Digispark + meterpreter payload - vesiluoma.com*. [online] Available at: <https://www.vesiluoma.com/exploiting-with-badusb-meterpreter-digispark/> [Accessed 30 Apr. 2019].

Highon.coffee. (2019). *Reverse Shell Cheat Sheet*. [online] Available at: <https://highon.coffee/blog/reverse-shell-cheat-sheet/> [Accessed 30 Apr. 2019].

Kaspersky.com. (2019). *Kaspersky Lab patents BadUSB cure*. [online] Available at: <https://www.kaspersky.com/blog/badusb-solved/12539/> [Accessed 2 May 2019].

Davidzou.com. (2019). *Defend Against BadUSB / davidzou.com*. [online] Available at: <https://davidzou.com/articles/windows/defend-against-badusb> [Accessed 2 May 2019].